Schegge di Cassandra/ OHM2013: Wireless 3G appeso ad un filo?

(297) - Infrastruttura rappezzata e nuove tecnologie che continuano a fare intrugli con il vecchio. E l'anello debole della catena è lì per…

Schegge di Cassandra/ OHM2013: Wireless 3G appeso ad un filo?

Figure 1:

(297) - Infrastruttura rappezzata e nuove tecnologie che continuano a fare intrugli con il vecchio. E l'anello debole della catena è lì per essere spezzato.

23 agosto 2013—Se una delle volta che estraiamo il cellulare dalla tasca ci soffermassimo a pensare a quanto abbiamo in mano, smartphone o dumbphone che sia, lo potremmo descrivere come il punto di accesso ad una vastissima rete di servizi telefonici e telematici. In effetti è una descrizione molto generica ma del tutto esatta.

Si è parlato molto (ma non abbastanza) dei problemi di privacy ed altro legati al fatto che i cellulari, permanentemente ed in vario modo connessi alla loro rete, potevano liberamente fornire informazioni sul loro possessore a chi controllava la rete mobile (2G, 3G, 4G) e a chi controllava il controllore. Cassandra in questo ha certo fatto abbondantemente la sua parte.

Bene, anche se vi sembrerà strano al limite dell'impossibilità, specialmente alla luce del Datagate (grazie Edward), Cassandra oggi trascurerà completamente tutto ciò e si concentrerà sull'altra metà del cielo, cioè sulla rete mobile stessa.

La finalità di ogni "Scheggia", è quella di riassumere e rendere meno tecnologico il contenuto di uno dei divini seminari di OHM2013, in questo caso quello tenuto da Philippe Langlois ed intitolato "Violare l'HLR: l'insicurezza delle infrastrutture delle reti mobili e critiche".

Ora, persino parecchi del 24 informatissimi lettori avranno avuto un momento di sbandamento di fronte all'ennesima sigla sconosciuta come HLR, che significa semplicemente Home Location Register.

In soldoni si tratta di un database centralizzato che contiene i dettagli di ogni abbonato autorizzato all'uso della rete mobile.

Un HLR contiene i dettagli di ogni SIM card fornita dagli operatori di telefonia mobile, perché ogni SIM contiene un identificativo univoco (IMSI), che è la chiave di ricerca che permette di recuperare nell'HRL tutti i dettagli sull'abbonato, il numero telefonico associato alla SIM, la matricola del telefonino utilizzato e vai così.

Di questi database ne esistono diversi, tutti coordinati tra loro, e la rete globale mobile è costituita da diversi tipi di apparecchiature quali NSS, HSS, MME, MSC…

Qualunque numero di cellulare esiste solo se è incluso in uno dei vari HLR sparsi in giro per il mondo e coordinati tra loro. Come in Matrix, quindi, chi controlla questo database controlla la realtà.

Ma non è questa la storia raccontata da Philippe o, almeno, ne costituisce solo lo sfondo. Infatti questo raggruppamento di database, reti di comunicazione, apparecchiature e protocolli che sta "aldilà" del nostro amato (amato!?!?!) cellulare viene visto dagli utenti come un servizio unico, ma è in realtà composto da diversi tipi di nodi specializzati, a partire da ciò che si trova dietro l'antenna di un cella fino al server di database dell'HLR ed ai sistemi di contabilizzazione degli utilizzi.

La nostra storia parte dal fatto che tutti i sistemi, di tutti i provider (dicasi tutti) si trovano a funzionare su quella che a tutti gli effetti è una rete paritaria, in cui tutti i nodi sono considerati attendibili. Parliamo di qualcosa molto simile ad una LAN, ma su scala globale, su cui lavorano sia i più grandi provider, sia l'ultimo fornitore di accessi cellulari di un paese africano, del subcontinente indiano o della foresta amazzonica.

Quanto è forte una catena di trust? Come le catene vere, quanto l'anello più debole. E dopo aver superato le barriere di sicurezza del più insicuro dei provider cosa rimane per accedere ai sistemi di tutti i provider di tutto il mondo?Nulla. Assolutamente nulla.E' sufficiente quindi individuare un exploit anche banalissimo, tipo una password debole o di default, e sei dentro la rete mobile globale con poteri illimitati: puoi ad esempio "annunciare" alla rete che il tuo cellulare "italiano" in realtà si trova in roaming in un altro paese, ricevendone telefonate e SMS.

Cassandra si trova un attimo in difficoltà perché quanto sopra sembra la (salutare) solita dose di paranoia spesso somministrata in queste righe.

E' tanto opportuno quanto doveroso il sottolineare che in questo caso sta semplicemente riassumendo la descrizione della realtà quale la riferisce un esperto (molto esperto) indipendente (molto indipendente) del settore.Fatta questa doverosa precisazione, possiamo procedere: tratteggiamo un'ulteriore parte del panorama.

Le reti mobili e 3G sono formate da cataste di protocolli di comunicazione, segnalazione ed autorizzazione risalenti agli anni '80, ed implementati da vari costruttori e gestori in maniera totalmente indipendente e molto diversa. Poiché gli implementatori sono solitamente i fornitori chiavi in mano di apparecchiature complete, le specifiche dell'implementazione sono proprietarie e riservate, ed il modello di sicurezza utilizzato è quello della "Sicurezza tramite Segretezza", dimostratamente falso ma anche abbondantemente usato nella storia passata e presente, essendo il naturale complemento del normale modello di business dell'industria ICT, particolarmente di quella non consumer.

Per questo chi può mettere le mani su questi bellissimi rack pieni di marchi e lucette (in fondo qualche sistemista non troppo pagato li dovrà amministrare), trova dentro di essi hardware dedicato insieme a processori standard con sistemi operativi eterogenei, in parte ridondanti ma anche no, che spesso comunicano tra di loro a livello applicativo con architetture pesanti ed un po' azzardate, formate da blob di codice C++, Java o di scripting.

Questo codice, come tanti altri prodotti dall'industria, viene accuratamente testato fino alla prima volta che funziona, e poi resta tal quale fino a quando non è necessario attaccargli qualche altro pezzo, realizzando quello che nel dialetto informatico degli anni '80 si definiva, in senso dispregiativo, un "kludge".

Chi lavora nell'ICT su piattaforme che evolvono nel tempo sa che, malgrado siano testate in maniera formale ed implementino specifiche altrettanto formali, la qualità del codice che le realizza è di solito bassa, che la documentazione del codice stesso è normalmente disallineata od inesistente, che nessuno si preoccupa di mantenere la qualità del codice esistente, e che infine la tipica decisione architetturale che viene normalmente presa per apportare modifiche è quella di mantenere l'esistente, attaccandoci sopra qualche cosa in qualche modo.

E questo non e vero solo a livello di codice, ma anche di protocolli. Per aumentare le prestazioni ed i servizi, anche il mondo del 3G evolve verso protocolli più potenti, completi ed eleganti.

Peccato che anche in questo caso il mantenimento dell'esistente (detto talvolta "retrocompatibilità") la fa da padrone, e quindi ogni nuovo protocollo ammette il precedente come caso particolare, con tanti saluti ai miglioramenti della sicurezza che il nuovo protocollo permetterebbe. L'uso del "vecchio" è scoraggiato ma comunissimo, particolarmente da parte di chi, come il provider africano di cui sopra, non abbia i soldi per acquistare apparecchiature nuove, fare verifiche di sicurezza e spesso nemmeno manutenzione e configurazione.

Per coloro che avessero voglia di verificare quanto appena detto consiglierei di studiare una rappresentazione a blocchi di quello che un apparentemente semplice protocollo come il Bluetooth ha ancora sepolto nelle sue viscere, cioè il protocollo RS-232 ed i comandi AT. Poi ci si meraviglia del perché ci sono voluti anni prima di avere auricolari Bluetooth che funzionassero con qualsiasi marca di telefonini.

Le due massime "funziona, quindi non lo toccare più" ed "il provvisorio diventa permanente" hanno forgiato le reti mobili come sono adesso, non diversamente dall'informatica industriale, dallo SCADA, dai sistemi d'arma e di sicurezza.In questa luce, e lasciandosi guidare da qualche esperienza maturata in 30 anni di ICT, quello che dice Philippe diviene assolutamente ragionevole e credibile.

La domanda che ci si potrebbe porre a questo punto è: perché le reti mobili e 3G non collassano ogni volta che uno script kiddie si stanca di guardare i cartoni in TV? Beh, innanzitutto ogni tanto, anche se solo in parte, collassano davvero, anche se nei comunicati stampa si parla sempre di "problemi tecnici" o di "disservizi limitati".

Poi parliamo di un cracking di alto profilo, per cui non basta scaricare i programmini dai siti dell'est europeo.

Non si deve nemmeno sottovalutare l'equilibrio del terrore: da un collasso di tutta od anche solo una parte della rete tutti gli attori hanno da perdere. Ecco dove la sicurezza tramite la segretezza può in parte funzionare: dove tutti i grandi attori hanno solo da perdere.

Ma per quanto? Quanto si può contare su un'infrastruttura del genere in caso di attacco ben finanziato o di guerra informatica? L'ENISA ha provato a dare un'idea dell'affidabilità

del sistema con il suo report annuale, ma è comunque difficile dare una risposta abbastanza pessimistica ma che non sia solo un'opinione.

Volendo sintetizzare, non si tratta di incompetenza, cattiveria o incoscienza, ma principalmente del fatto che a tutti i livelli della produzione di software, dall'elettronica di consumo fino ai sistemi gestionali di una grandissima azienda, si vende quello che l'acquirente vuole, e sono le funzionalità di base che pagano, dalle suonerie e SMS fino al numero di connessioni servite da una cella, non una sicurezza infrastrutturale collaudata e dimostrabile.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on March 22, 2023.

Canonical link

Exported from Medium on August 27, 2025.